# Lexmark Security Advisory:

Revision: 1.1
Last update: 19-July-2021
Public Release Date: 9-Feburary-2015

## *Summary*

Input Sanitization vulnerability

Markvision Enterprise contains a vulnerability that allows uploaded ZIP files to be unpacked into arbitrary locations.

## *References*

CVE: CVE-2014-9375

## *Details*

Markvision Enterprise contains a servlet named "LibraryFileUploadServlet". This servlet allows an authenticated user to upload ZIP files that, when unpacked, can use directory traversal to write files in arbitrary locations on the Markvision Enterprise server, including the ability to upload and execute code with the privilege of the Markvision Enterprise application.

## *Impact*

Successful exploitation of this vulnerability can lead to the disclosure of data stored in Markvision Enterprise, and the ability to execute code within the Markvision platform.

## *Vulnerability Scoring Details*

CVSS Base Score 9.0
Impact Subscore: 10
Exploitability Subscore: 8.0

| Exploitability: | | Impact: | |
|---|---|---|---|
| Access Vector: | Network | Confidentiality: | Complete |
| Access Complexity: | Low | Integrity: | Complete |
| Authentication: | Single | Availability: | Complete |

CVSS scores are calculated in accordance with CVSS version 2.0 (http://www.first.org/cvss/cvss-guide.html)

## *Workarounds*

Lexmark recommends updating the application if you have a vulnerable version.

Please visit http://www.lexmark.com/markvision or contact the Lexmark Technical Support Center at 1-800-539-6275 for additional information.

### *Software Versions and Fixes*

The vulnerability described in this advisory has been fixed in Markvision Enterprise v2.1.1 and all future releases. All releases previous to v2.1.1 are vulnerable.

## *Obtaining Updated Software*

To obtain Markvision Enterprise v2.1.1, please visit http://www.lexmark.com/markvision.

## *Exploitation and Public Announcements*

Lexmark is not aware of any malicious use of the vulnerability described in this advisory.

Lexmark would like to thank rgod working with HP's Zero Day Initiative (ZDI) for bringing this issue to our attention.

## *Status of this Notice:*

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND IS PROVIDED WITHOUT ANY EXPRESS OR IMPLIED GUARANTEE OR WARRANTY WHATSOEVER, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR USE OR PURPOSE. LEXMARK RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

## *Distribution*

This advisory is posted on Lexmark's web site at http://support.lexmark.com/alerts
Future updates to this document will be posted on Lexmark's web site at the same location.

## *Revision History*

| Revision | Date | Reason |
|---|---|---|
| 1.0 | 26-January-2015 | Initial Public Release |
| 1.1 | 19-July-2021 | Updated legal notice |